Data Protection Policy

Policy no:	6.0	**Version number**	V1.4
Version date	Oct 2024	**Next review**	Oct 2025
Owned by	Chief Executive Officer	**Approved by**	Senior Leadership Team
Key contacts	Data Controller: academics@lckacademy.org.uk Data Protection Officer: Head of IT shafraz@lckacademy.org.uk		
External reference points	Data Protection Act 25 May 2018 Information Commissioners Office (ICO) If you operate inside the UK, you need to comply with the Data Protection Act 2018 (DPA 2018). The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations GDPR 7 Principles • Lawfulness, fairness and transparency. • Purpose limitation. • Data minimisation. • Accuracy. • Storage limitation. • Integrity and confidentiality (security) • Accountability. OfS Condition C1 The provider must demonstrate that in developing and implementing its policies, procedures and terms and conditions, it has given due regard to relevant guidance about how to comply with consumer protection law. UK Quality Code for Higher Education 2024 Principle 4 When designing and operating monitoring and evaluation arrangements, staff and students adhere to ethical and data protection requirements relating to gathering and submitting data for national data sets, regulatory purposes, and internal monitoring and evaluation.		

Contents

1. Background and Purpose 3
2. Aims and Objectives 3
3. Application 3
4. Rationale and Scope 4
5. Staff 4
   5.1. Keeping staff records: the legal requirements 5
   5.2. Other staff records that should be kept 5
   5.3. The level of detail in employee records 6
   5.4. How long to retain staff records? 6
   5.5. Statutory record retention period 7
   5.6. Recommended record retention period 8
6. Requirements of the Data Protection Act 9
7. Warning 9
8. Data Controller and Data Protection Officer 9
9. Notifying the Information Commissioner`s Office (ICO) 10
10. Employees` rights of access to data 10
11. Additional guidance on Data Protection issues 11
12. Responsibilities under the Data Protection Act 11
13. Consent 11
14. Disclosure and Disposal of Data 12
15. Informing Students of Disclosures and Obtaining Consent 14
16. Method of Disclosure 14
   16.1. Disclosure to Work Colleagues 14
   16.2. Disclosure to Relatives/Guardians and Friends 15
   16.3. Confirmation of Student Status and Award 16
   16.4. Disclosure to Sponsors (includes Student Loan Company and Research Councils) 16
   16.5. Disclosure to the Student Loan Company 17
   16.6. Disclosure to current and prospective Employers and Educational Institutions 17
   16.7. Requests for Personal References 17
   16.8. Disclosures to the Police 18
   16.9. Legal Proceedings 19
17. Use of CCTV 19
18. Academic Research 19
19. Monitoring and Evaluation 19

1. Background and Purpose

LCK Academy ('LCKA' or 'the Academy') is dedicated to safeguarding the privacy and rights of all individuals, including students, visitors, employees, governors and all other stakeholders. In accordance with the Data Protection Act 2018, the Academy limits the amount of data it keeps on individuals to only that which is necessary to fulfil its purpose and meet its legal and regulatory requirements as a higher education provider. To this end, the Academy proactively mitigates the risk of data breaches to protect the rights of individuals whose data is under our care, otherwise referred to as the 'data subjects'. This policy should be read in conjunction with the following LCKA Policies: Your Rights about Your Data, and Data Privacy Notice and Consent Policy.

2. Aims and Objectives

This policy aims to ensure that the Academy is compliant with the UK Data Protection Act 2018 (DPA). The following EU GDPR principles that are incorporated within this Act, constitute the key objectives of this policy as listed in the GDPR 7 Principles:
:

- To process personal data of individuals lawfully, fairly and transparently.
- To ensure that the personal data of individuals is only used for the reasons it was originally collected and for no other purpose without the permission of the individuals concerned.
- To ensure that the amount of personal data the Academy holds is no more than the minimum required for the Academy to fulfil its purpose.
- To take reasonable steps to ensure that all personal data the Academy holds on individuals is correct, updated when required and not misleading.
- To only store personal data on individuals for as long as is necessary for processing. There is no specified time limit, but the Academy will delete all personal data it stores when it is no longer needed for the purposes it was originally collected.
- To ensure that all data the Academy holds is secure and confidential and that only those who need it have access to it.
- To appoint an accountable Data Controller for the Academy. The Data controller is responsible for deciding how and why data is processed and is responsible for ensuring that the Academy is compliant with the DPA and these GDPR principles.

3. Application

The policy applies to all staff, students, governors and other stakeholders of the Academy. The Academy expects all stakeholders to comply with this policy as they are legally required to comply with the Data Protection Act 2018 (DPA). If there is any breach of this policy or the DPA, LCK Academy disciplinary measures will be implemented as indicated in the Staff Handbook, or the Fitness to Study Policy.

Other organizations and people who collaborate with the Academy and have access to or process personal data will be expected to:

a) Have their own Data Protection Policy that covers all the relevant requirements that this policy covers, or
b) Read and comply with this policy.

Staff and Academy representatives who work with external organisations or individuals that process personal data in collaboration with the Academy are responsible for ensuring that those organisations or individuals are compliant with points (a) and (b) above. Any partnership where the personal data of individuals will be processed, LCKA, and partner of LCKA or both parties may be responsible for ensuring policy compliance and reporting on this to the Academy's Data Controller. This may require the LCKA Data Controller to read and comment on the Data Protection Policy of its partner organisation.

4. Rationale and Scope

For administrative purposes, the Academy must process specific data about its students, employees, and other parties with whom it interacts. This includes (but is not restricted to) the recruitment and payroll of staff, administration of programmes of study, recording student continuation, completion and progression as defined by HESA, conferment of awards, collection of fees, and compliance with legal obligations regarding the processing of data for the purposes and requirements of student finance including student loan funding. Information about individuals must be gathered and utilised appropriately in accordance with seven GDPR Principles provided in the Aims and Objectives above. Data entrusted to the Academy must be minimal and held securely for no longer and for no other purposes than it was originally intended. It is unlawful to hand personal data of individuals to third parties without the data subject's permission, apart from circumstances where the Academy is otherwise legally obligated to do so.

5. Staff

This policy guides the retention of staff records and outlines the Academy's legal responsibilities as an employer, as well as the rights of employees concerning their personal information. There are distinct legal, safety, and commercial reasons for retaining and proactively securing the integrity and safety of personal data on the staff that the Academy employs. In documenting employee personal data, Academy staff, especially those responsible for human resource management should be fully conversant with all the requirements and expectations of the DPA as set down in this policy. They should exercise extreme caution when processing the personal data of staff.

In particular, stakeholders who process the personal data of Academy staff should be aware of the following conditions in the Data Protection Act 2018 (DPA):

- The Academy is obligated to proactively update the accuracy and relevance of all personnel details it retains in a timely fashion. This includes deleting data that is no longer needed for the purposes it was originally collected unless otherwise requested or permitted by the individual(s) concerned.
- Employees may request access to the personal data that the Academy holds on them.
- Employees may claim compensation for any detrimental effect they may have suffered as a result of a violation of the DPA.

5.1. Keeping staff records: the legal requirements

The Academy is legally required to maintain staff details on:

- Hours spent to comply with the Working Time Regulations, as well as employees who have consented to work more than 48 hours
- Pay rates, to guarantee compliance with the National Minimum Wage Act of 1998, and fulfil the legal obligation to provide pay statements to employees
- Payroll Administration data such as national insurance and income tax deductions for HM Revenue & Customs
- More than four days of illness and the amount of statutory sick pay received
- Accidents, injuries, and hazardous near misses at work to adhere to health and safety regulations
- Bank account numbers for processing payments
- Background criminal checks and information about any crimes committed
- Pension details

5.2. Other staff records that should be kept:

Records of every employee also include:

- Name, location, emergency phone number(s), credentials, and any disabilities that are relevant to the job
- Employment terms and conditions, together with a copy of every employee's written correspondence and terms and conditions about any modifications
- Employment history including start date, job title(s), and promotions
- Documentation of absences, whether authorized or not, including lateness and illness
- Staff performance reviews, lesson observations and CPD records

Additional general records include:

- Attendance and contributions at meetings
- Any sanctions imposed as well as the minutes of any hearings related to sanctions
- Meetings and agreements for individual and group consultation on redundancies
- Information and consultation agreements are the subject of negotiations.

5.3. The level of detail in employee records

The Data Protection Act 2018 stipulates that personal data retained on employees must be minimised to what is sufficient for the purpose it was collected. When recording absence rates, employee turnover, illness, lateness, and staff discipline, the Academy will require adequate records and the system for processing and recording such data must be efficient and secure.

Not all records can be kept electronically. Signed copies of some vital documents may also be kept in locked filing cabinets. This is particularly needed if the Academy is ever called to an employment tribunal. The Academy adheres to the following data security good practices:

- All hard copy of personal data of staff is filed and stored in locked cabinets or drawers.
- Only employees who require access to personal data on other employees have access it.
- Electronic documents are secured with firewalls, anti-virus programmes, and passwords
- If required, an audit trail tool is used to track who has viewed a specific record and when.

5.4. How long to retain staff records?

It is customary to keep staff records for six years to accommodate the statute of limitations for filing any civil lawsuit against the Academy, including claims related to contractual obligations and the federal minimum wage. More detailed instructions for certain record types are provided in the accompanying table.

5.5. Statutory record retention period

Documents/Data	Retention Period
Accident reports	Three years after the date of last entry. Io t may be required to retain records of incidents involving hazardous substances (COSHH) for up to 40 years.
Payroll records	At least three years after the end of the tax year that they relate to.
Statutory maternity, adoption and paternity pay records	Three years after the end of the tax year they relate to.
Statutory sick pay records	Three years after the end of the tax year they relate to.
Working time	Two years from the date on which they were completed.
National minimum wage records	Three years after the end of the pay reference period that follows the period the records cover.
Retirement benefits schemes and notifiable events, e.g., relating to incapacity	Six years from the end of the year in which the scheme started or event took place

5.6. Recommended record retention period

Documents/Data	Retention Period
Application forms/interview notes for unsuccessful candidates	One year
Health and safety records of consultations	Permanently
Parental leave taken	Five years from birth/adoption, or until the child is 18 if disabled
Pensioners' records	12 years after the pension ceases
Disciplinary, working time and training records	Six years after employment ceases
Redundancy details	Six years from the date of redundancy
Senior executives' records	Permanently for historical purposes
Trade union agreements	Ten years after ceasing to be effective
Minutes of trustee/work council meetings	Permanently
'Right to work' documents	Two years after employment ceases

According to the Data Protection Act of 2018, information should not be held for longer than is required for a specific reason. Data should be safely and effectively disposed of when it is no longer needed, for example, by shredding. Until being disposed of, information about current and past employees should, whenever feasible, be stored anonymously.

6. Requirements of the Data Protection Act

Personal data, or information about living, identifiable individuals kept electronically or in manual filing systems, is covered by the Data Protection Act of 2018. The Act's guidelines for handling such data are based on eight distinct concepts.

The following guidelines should be followed by all Academy stakeholders when handling data:

- Process it fairly and legally, ensuring that staff members understand the purpose of collecting the data and how it will be used.
- Avoid using information for purposes other than those for which it was intended; do not give personal information to third parties unless you are sure it is permitted and required.
- It should be no more than sufficient, relevant, and not in excess of what is required for its stated purpose.
- It should be precise and updated as needed, but not retained for any longer than necessary
- It should be processed according to people's rights, such as their right to access; and kept secure by taking the necessary organisational and technical precautions to safeguard the data.
- It should not be transferred to nations outside of the European Economic Area unless it is sufficiently protected and permission has been granted by the individual(s) concerned.

These principles should be addressed when selecting what information to gather, developing methods for processing the information, and responding to requests for access to the information.

7. Warning

Failure to comply with the Data Protection Act 2018 and its data protection principles may result in an enforcement notice from the Information Commissioner's Office (ICO). The violation of a notice is a criminal offence. Employees and others can seek compensation if they suffer damage (typically physical or financial) or other detrimental effect as a result of the company's violation of the Data Protection Act 2018.

8. Data Controller and Data Protection Officer

LCK Academy Ltd trading as LCK Academy is registered with the Information Commissioner's Office as a data controller (Registration reference: ZB562779). LCKA's Data Protection Officer is its Head of IT shafraz@lckacademy.org.uk. The DPO keeps up to date on all data protection law and practices as outlined by the Information Commissioner's Office. The DPO is responsible for ensuring that all relevant staff and stakeholders including the Data Controller, HR Manager and Registry Officer complete General Data Protection Regulation (GDPR) training. The Academy requires staff to complete their training through reputable providers such as iHasco here

9. Notifying the Information Commissioner`s Office (ICO)

According to the Data Protection Act 2018 and the seven data protection principles provided in the Aims and Objectives above, the Academy Data Protection Officer (DPO) is obligated to notify the Information Commissioner's Office (ICO) regarding the processing of personal information, except where exemptions apply. The ICO provides guidance on this notification process and compliance with data protection legislation. Failure to notify the ICO, unless exempt, constitutes a criminal offence.

10. Employees` rights of access to data

Individuals have several rights under the Data Protection Act of 2018, including the ability to access any information held about them. If an employee requests any such information (a subject access request), they must submit the request in writing by email to the Data Protection Officer. The Academy may charge up to £10 for delivering the information and must respond within 40 calendar days.

Subject access requests (SAR) do not require the Academy to give the following information:

- Information stored for management planning, such as plans to promote or make an employee redundant.
- Information about the Academy's intentions when negotiating with the person requesting subject access if the employer (Academy) can demonstrate that complying with the SAR would likely prejudice the negotiations.
- References you have provided about the employee in confidence (references obtained by you are not exempt)
- Information concerning the prevention or detection of a crime, or the arrest or prosecution of criminals.
- Information that could identify someone else.

In addition to the right to access data about themselves, an employee has the rights to:

- Request the correction of inaccurate personal data.
- Seek compensation for damages incurred due to any violation of the Data Protection Act (DPA).
- Prevent data processing that is likely to cause significant damage or distress.
- Be informed of the rationale behind any automated decision made about them (if relevant), such as those resulting from psychometric testing.

If an employee has reasonable grounds to believe they have not been paid the national minimum wage, they have the right to review their pay records. They must submit a formal request, and the records must be produced within fourteen days.

11. Additional guidance on Data Protection issues

ACAS helpline
08457 47 47 47

National Minimum Wage helpline
0845 6000 678

Information Commissioner's Office Data Protection helpline
01625 545 745

Health & Safety Executive Infoline
0845 345 0055

Information Commissioner's Office Notification Line
01625 545 740

12. Responsibilities under the Data Protection Act

Compliance with data protection legislation is the duty of all Academy members who handle personal information of individuals. Staff at the Academy are responsible for ensuring that any personal information provided to the Academy is accurate and up to date.

13. Consent

Personal or sensitive data should not be gathered, retained, utilised, or disclosed without the individual's consent. The Academy defines "consent" as the data subject being fully informed of the intended processing and indicating their acceptance whilst in a fit state of mind and without being pressured to do so.

Consent acquired under duress or based on misleading information will not be considered legitimate for processing. There must be some active contact between the parties, such as signing a form, and the individual must do it freely and willingly. Non-response to a communication does not constitute consent. For sensitive data, specific written consent is required from data subjects unless a legal or regulatory obligation for processing the data exists.

In most cases, the Academy routinely obtains consent to process personal and sensitive data (e.g., when a student signs a registration form or a new staff member sign an employment contract). **Any Academy forms, whether paper-based or online, that collect data on an individual must include a statement explaining the purpose of the data collection and to whom the information may be disclosed.** It is especially important to obtain explicit consent if an individual's data is to be published on the Internet, as such data can be accessed globally.
Failing to obtain consent could violate the seventh data protection principle as described in the Aims and Objectives above.

If an individual does not consent to certain types of processing (e.g., direct marketing), appropriate measures must be taken to ensure that the processing does not occur. If any member of the Academy is uncertain about these matters, they should consult the Academy Data Protection Officer or refer the issue to the Senior Leadership Team.

14. Disclosure and Disposal of Data

The Academy must ensure that personal data remains confidential and is not shared with unauthorised parties, including family members or friends. All staff and students are advised to exercise caution when requested to divulge personal information about another individual to a third party. For example, it may be appropriate to provide a colleague's work contact information in response to an inquiry related to their professional responsibilities. However, disclosing such details for non-work-related purposes would generally be considered inappropriate. The key consideration should be whether the information requested is relevant and necessary for Academy-related activities. Ideally, individuals should take the contact information of the inquirer and relay it to the relevant Academy member as best practice.

This policy outlines the legitimate conditions under which personal data may be disclosed:

- **Consent**: Personal data can be disclosed if the individual data subject has given explicit consent. For example, a student or staff member may allow the Academy to share their information with a specific third party.
- **Legitimate Interests**: Personal data may be disclosed if it is in the legitimate interests of the Academy. For instance, personal information can be shared among Academy employees if they require this to perform their job effectively.
- **Legal Obligation**: The institution may be legally required to disclose data in certain situations. Examples include sharing data with bodies like HESA, HESES, SLC, HEFCE, and for ethnic minority and disability monitoring purposes.
- **Contractual Obligation**: Data may be disclosed if it is necessary for fulfilling a contract. For instance, informing a student or their sponsor about course changes or withdrawal.

The Data Protection Act 2018 allows certain disclosures of information without consent if they are requested for the following purposes:

- Safeguarding national security.
- Prevention or detection of crime, including apprehending or prosecuting offenders.
- Assessment or collection of tax duty.
- Carrying out regulatory functions, which include ensuring health, safety, and welfare at work.
- Preventing serious harm to a third party.
- Protecting the vital interests of an individual, particularly in life-threatening situations.
- Maintaining effective immigration control should the Academy recruit international students or staff on work visas.

When staff members receive inquiries regarding the status of a specific individual in the Academy, they are required to inquire about the purpose of the request. If consent for disclosure has not been granted and the purpose does not fall within the predefined exceptions (i.e., situations where consent is not necessary), staff members should refrain from providing any information. Even confirming or denying an individual's status at the Academy as a student, member of staff or otherwise could potentially be considered an unauthorized disclosure.

Unless the data subject has given consent, no information should be released over the phone. Instead, the requester should be asked to show documentary evidence to back up their request. Ideally, the request should include a declaration from the data subject consenting to disclosure to the third party.

Instead of sharing personal information, the Academy can offer to undertake one of the following:

- Send the data subject a message requesting that they get in touch with the requester;
- When an email or sealed envelope arrives, accept it and try to forward it to the data subject.

Please ensure to notify the requester that an individual's status at the Academy cannot be confirmed or denied without their permission, if they are available to grant permission. This approach prevents confirmation of their status, presence, or absence at the institution.

Personal data must be disposed of at the appropriate time on approval by the Data Controller in a way that safeguards data subjects' rights and privacy (such as shredding or secure electronic deletion). See the Statutory Retention and Recommended Retention Periods in the tables above.

In cases of uncertainty, employees are advised to seek guidance from their line manager first, then the Data Protection Officer, and finally the Data Controller.

15. Informing Students of Disclosures and Obtaining Consent

When students register with the Academy, they should be advised of expected disclosures (such as confirmation of student status or response to a request for a reference). Some students may choose to opt out of some processes (including disclosures) on their registration form. This information is stored in the Academy database, and all staff members should review a student's record before disclosing any information.

- In less predictable instances (e.g., a family member calling for financial information, a taxi company that has discovered a wallet and wants to contact the student), if the student has not been previously advised of a potential disclosure, the student should provide their approval before any information is disclosed.
- The Academy defines "consent" as the student's agreement while in a fit state of mind and without being pressured. Consent cannot be inferred from a failure to respond to a communication; active contact between the parties is required. Verbal consent is typically permitted with sufficient security checks to confirm the student's identity. For telephone consent, ask the subject to affirm numerous independent facts that should be kept private (student number, date of birth, etc.).
- There are several exceptions (Section 29 of the Freedom of information Act and Section 29(1) of the Data Protection Act 2018) to the requirement to notify students of disclosures if the information is being revealed for the prevention or detection of crime AND alerting the student will jeopardize the investigations.

16. Method of Disclosure

Disclosures should not be conducted over the telephone. The recommended procedure is for the requester to leave their contact information and for the respondent to initiate a return call. It is highly recommended that all requesters submit their inquiries in writing, preferably on official letterhead where applicable. Following verification of the legitimacy of the request, responses should, whenever feasible, be provided in written form.

16.1. Disclosure to Work Colleagues

Caution should always be exercised when disclosing students' personal information to colleagues. According to the Data Protection Act 2018, personal data should not be shared with colleagues unless there is a legitimate reason for the data. The determination of what constitutes a "valid reason" is context-dependent and should be evaluated on a case-by-case basis.

A guiding principle is to consider whether the information is essential for colleagues to effectively fulfil their job responsibilities. For example, sharing student addresses, degree classifications, and information about disabilities would be appropriate if special accommodations are required for the student's participation in a graduation ceremony. Similarly, sharing relevant information with course tutors for teaching purposes or seating arrangements is permissible.

When disclosing information, it is important to assess the level of detail necessary for colleagues to carry out their duties. For instance, notifying colleagues about a student's extended absence may be appropriate, while the specific reasons (such as health-related issues) for the absence may not need to be disclosed to all colleagues.

16.2. Disclosure to Relatives/Guardians and Friends

- The Academy is not permitted to share any personal information about students with their relatives without permission from the data subject, even if the relatives are contributing to tuition fees, unless there are extenuating circumstances that may necessitate the disclosure of data as detailed above under Disclosure and Disposal of Data.

- Always verify whether the third party is using the correct password from the student's record. There may be pressure to discuss individual students with parents, guardians, or friends. However, it's crucial not to disclose personal data without the student's prior consent, as this would violate the Data Protection Act 2018. If the student has given their password to a third party, it implies they have given consent.

- Once consent has been established, staff can discuss institutional procedures with relatives, such as explaining reassessment procedures, and graduation ceremony dates, or advising on payment deadlines. Confirmation of consent is also required for discussing the specific circumstances of a student.

- In rare, urgent situations (such as threats to a student's life or health), the usual requirement for consent before disclosing information to relatives including parents or guardians may be waived by members of the Senior Leadership Team. The Academy keeps records of students' "next of kin" for such emergencies.

16.3. Confirmation of Student Status and Award

Student status constitutes personal data and must be handled under the provisions of the Data Protection Act 2018. This entails ensuring that the information is protected from unauthorized disclosure. Verifying whether an individual is or has been enrolled at the Academy may potentially breach the Act.

The Academy may receive inquiries regarding the status of individual students. Such requests may originate from various parties, including current or prospective employers seeking to verify details on job applications, as well as estranged or abusive partners attempting to locate individuals. Consequently, caution should be exercised before responding to requests for confirmation of student status.

Typically, requests are made by entities with a legitimate interest in the information. As part of the registration process, students are informed that information regarding their student status and final award may be disclosed to the Home Office, Police, and prospective or current employers and educational institutions upon request. Students are provided with the option to withhold consent for such disclosures, necessitating verification of student records before providing any information. It is imperative to employ appropriate security measures to authenticate the identity of the requester and refrain from disclosing information over the phone. Whenever feasible, it is requested that inquiries be submitted in writing, preferably with an official letterhead.

In cases involving other inquiries, confirmation or denial of an individual's student status should not be provided without their explicit consent, unless compelled to do so by statutory or legal obligations.

16.4. Disclosure to Sponsors (includes Student Loan Company and Research Councils)

Students are provided with the opportunity to indicate their objection to the disclosure of attendance and achievement information to sponsors via their registration forms. Before sharing any information with a sponsor, it is necessary to verify that the student has not exercised this option by checking their record.

16.5. Disclosure to the Student Loan Company

The Student Loan Company (SLC) evaluates the eligibility of undergraduate students for student loan payments. The initial assessment is conducted directly between the student and the SLC, without the Academy's involvement. However, the SLC does require confirmation of students' registration status and course attendance from the Academy. This disclosure is mandated by law, and students are made aware of this requirement during their registration process.

When disclosing information to the SLC, the Academy only shares factual information. If sensitive data, such as health-related information, needs to be disclosed to the SLC, student consent is required. If students access SLC funding through one of the Academy's partner awarding organisations, such as a university or college, the Academy will provide the necessary information to the partner organisation, who will then pass it to the SLC.

16.6. Disclosure to current and prospective Employers and Educational Institutions

Requests for information regarding individual students, whether current or former, may be received from current or prospective employers and educational institutions. Such inquiries commonly occur during a student's application for employment or enrolment in a course. Generally, these disclosures are made in the best interests of the student, who is typically aware of the possibility of such requests.

The information disclosed in response to these inquiries should be limited to essential details, such as the student's enrolment status and any academic achievements received. These disclosures are considered routine, and students are informed about them during the registration process, with an opportunity to opt-out if they choose to do so. Before releasing any information, it is crucial to verify the student's record to ensure that they have not opted out of this disclosure process. Careful consideration should always be given to the manner in which information is shared to protect student confidentiality and privacy.

16.7. Requests for Personal References

When providing a personal reference for a student, it is important to verify the information is accurate and in circumstances where possible, it is advisable to limit disclosure.

- Information considered sensitive, such as details regarding health-related absences from the Academy, ought not to be shared unless the student has expressly consented.
- Statements concerning an individual's suitability should be based on justifiable and reasonable grounds.
- If unable or unwilling to furnish a reference, it is appropriate to decline discreetly without implying a negative assessment or disclosing personal information.
- When asked to provide an unsolicited reference for a student who has not designated you as a referee, refraining from divulging any information is recommended.

The identity of the individual requesting the reference should always be verified before disclosure. Requests for references are typically expected in an email request. It is essential to ensure its authenticity, especially if it originates from an unfamiliar domain. If the request originates from a recognised source or domain associated with a known entity, the reference can be sent.

Telephone references are generally discouraged unless expressly requested by the student for urgent submission. In such cases, it is recommended to verify the caller's identity by returning their call before providing any information.

Students are informed upon registration that their student status and degree credentials may be verified for potential employers. They have the option to opt-out, and this choice is duly recorded in their student file. The Student Handbook specifies that student records are retained post-graduation to accommodate requests from prospective employers, provide references, and furnish evidence of assessed work to accrediting bodies, adhering to the retention periods mandated by partner organisations and accrediting bodies, typically ranging from 3 to 6 years apart from information on awards, which is held indefinitely. The Academy may retain records longer than 6 years to support alumni needs, although such extended retention is not guaranteed. For replacement of lost or damaged certificates, students are advised to contact the respective awarding organisation, such as a university, college, or Pearson.

If a student designates a staff member as a referee, it is presumed that implicit consent for information disclosure has been granted, irrespective of their registration opt-out status. Should a staff member be unaware of being designated as a referee, they are advised to verify the legitimacy of the request before proceeding.

16.8. Disclosures to the Police

The Academy is not obligated to disclose information to law enforcement authorities unless it receives a court order compelling such disclosure. Nevertheless, certain exceptions to this rule are permitted under Section 29 of the Data Protection Act 2018. These exceptions allow the Academy to divulge information to the police without students' consent in specific circumstances. Such disclosures are permissible only when the police request to interview a specific individual in connection with a criminal investigation, and when the Academy believes that withholding the information could potentially compromise the investigation.

It is prohibited for staff members to provide information to the police via telephone. Instead, the police must submit a written notification to the Academy. This notification should include a statement affirming that the requested information is necessary under the provisions outlined in Section 29, a brief overview of the nature of the investigation, the student's involvement, and the signature of the investigating officer. This procedure is standard across the majority of police forces.

16.9. Legal Proceedings

Section 35(2) of the 1998 Act provides an exemption from non-disclosure requirements, such as obtaining student consent, under specific circumstances. These circumstances include disclosures made for legal proceedings, obtaining legal advice, or when necessary for establishing, exercising, or defending legal rights. Consequently, the Academy is permitted to disclose student information to its solicitors when seeking legal advice. However, information about cases unrelated to the University should only be disclosed with the explicit consent of the relevant student. In cases where a court order mandates the disclosure of information, Section 35(1) explicitly authorises data controllers to disclose such information without requiring consent from the student.

17. Use of CCTV

The community college and local borough council facilities that are used by the Academy to deliver its services have CCTV cameras installed for security purposes. All CCTV recordings of students, staff and other stakeholders are retained by staff responsible for the security of the premises. LCKA will adhere by the security policies in place to protect individuals from harm. Video recordings will not be shared with third parties except when there is an emergency or there is a legal obligation to do so if, for example, there is an allegation that a crime may have been committed on the premises.

18. Academic Research

The Academy Research Ethics Committee (REC) is responsible for ensuring that any Academic research undertaken at the Academy complies with the British Educational Research Association (BERA) guidelines for ethical research, which includes protecting the anonymity of individual participants and obtaining consent to use their personal information. Research at the Academy may be conducted by staff or students as part of their undergraduate studies. Research may involve surveys, interviews, focus groups or observations of participants. The Academy ensures that all data on individuals is anonymised and their consent is obtained before it is used for any publication. Refer to the LCKA Research Ethics Policy for more information.

19. Monitoring and Evaluation

The Data Protection Officer (DPO) monitors the implementation and effectiveness of this policy and provides an evaluation of findings to the Data Controller, who chairs the Academy Advancement Committee. The Data Controller reports on the impact of this policy to the Senior Leadership Team on a quarterly basis. The DPA also provides an annual review on Data Protection at the Academy which contributes towards the Academy's Internal Academic Monitoring Review.